MULTIMEDIA UNIVERSITY

FINAL EXAMINATION

TRIMESTER 2, 2016/2017

TIA2221 – INFORMATION ASSURANCE & SECURITY
(All Sections / Groups)

4 MARCH 2017
2.30 p.m – 4.30 p.m
(2 Hours)

INSTRUCTIONS TO STUDENT

1. This Question paper consists of 3 pages with 5 Questions only.

2. Attempt **ALL** questions. All questions carry equal marks (10) and the distribution of the marks for each question is given.

3. Please print all your answers in the Answer Booklet provided.

Question 1

1a)   State the relationship between Threat, Vulnerability and Attack?

[3 Marks]

1b)   Define "A Black Hat Hacker" and describe how hackers create security problems and damage systems.

[3 Marks]

1c)   List and describe any of the **FOUR** most common threats against contemporary information systems.

[4 Marks]

Question 2

2a)   Explain why are non-malicious insiders considered as threats?

[2 Marks]

2b)   Explain the term "Passive Assessment" in network security assessment with an example.

[2 Marks]

2c)   One of the key challenges for assessment of security assurance is verifying conformance with security requirements. Another is assessing how effective business units have been in enforcing security conformance.

Explain any **THREE** key metrics needed to verify conformance with security requirements.

[6 Marks]

Question 3

3a)   Describe with **TWO** examples when does a person become an information security risk?

[4 Marks]

3b)   The Chief Information Security Officer of an organisation requested the Human Resource Manager to perform background checks on all IT personnel before hiring. It is necessary to perform background checks on all IT personnel?
State your reasons.

[3 Marks]

3c)   State **THREE** examples of external contingencies that need to be considered in a Computer Networked Operations (CNO) organisations.

[3 Marks]

Continued...

Question 4

4a)　　Explain how contingency theory is used to improve performance of an organisation.

[2 Marks]

4b)　　Hard disk and file analysis are one of the core activities in digital forensics to identify fraud .In terms of digital forensics; explain the importance of metadata and the main problem with using metadata as evidence.

[4 Marks]

4c)　　Explain the term "Identity Theft" with examples and why identity theft is such a big problem today.

[4 Marks]

Question 5

Suppose you are the security officer entrusted in assessing information security relating to a music festival. The organiser sells tickets online and post them once payment is accepted. You are only concerned with the risk of someone creating fraudulent ticket orders. You are not concerned with other risks such as leaking personal information.

5a)　　How would you prepare a risk assessment in this situation?

[6 Marks]

5b)　　Can you discover the highest **TWO** risk factors to be for the above scenario.

[2 Marks]

5c)　　Use your knowledge in 5a) and suggest **TWO** ways how these risks can be controlled?

[2 Marks]

End of Paper